Remarks/Arguments

Claims 1-22 are pending. Claims 1, 5, 13, 17, 19 and 21 have been amended to more clearly and distinctly claim the subject matter that applicants regard as their invention. Specifically the claims have been amended to more clearly recite verifying that a device, for example, a sink device, is authorized to receive protected content in response to a comparison of an approval code, or an identifier, with a local code, or set of security keys. Support for the amendment is provided, for example, on page 4, lines 2-6 and page 5, lines 13-16. No new matter is believed to be added by the present amendment.

Rejection of claims 1-21 under 35 USC 102(e) as being anticipated by Graunke (US Pat No 6731758B1)

Applicants submit that for at least the reasons discussed below Graunke fails to disclose or suggest each and every limitation of amended claims, 1, 5, 13, 17, 19 and 21, and thus, these claims, and the claims that depend therefrom, are not anticipated by Graunke.

The present invention is directed to a method and a system for **authenticating access** to otherwise protected content. Authenticating access refers to the notion of **verifying that a particular device is authorized** to receive the otherwise protected content. The authentication is distinct from the process of scrambling content for transmission, and is generally performed prior to communicating the protected content to a sink device.

Specifically, the present invention provides for a system that compares an approval code associated with a source device and a sink device with a local code generated using data associated with the source device and the sink device, and verifying that the sink device is authorized to received the content from the source device in response to the comparison. In an alternative embodiment, an identifier associated with a device is compared with a plurality of security keys, and authenticating access of the device is based on the comparison. In this regard, claim 1 has been amended to recite:

> ... comparing, in said source device, at least a portion of said approval code to at least a portion of said local code, and **verifying that the sink device is authorized to receive the protected content** from said source device **in response to the comparison**. (emphasis added)

Applicants submit that nowhere does Graunke disclose or suggest the above-mentioned limitation of amended claim 1.

By contrast, Graunke is primarily directed to a method and a system for **ciphering and deciphering** protected content, rather than authenticating access for verifying that a device is authorized to receive protected content. Graunke mentions that authentication is performed by an exchange of device identifiers and the respective devices and generating a common secret authentication key using the device identifiers and a random number (col. 3, lines 6-22). However, nowhere does Graunke disclose or suggest authentication by receiving an approval code associated with the source and sink devices, generating a local code using data associated with the source and sink device, and comparing the approval code with the local code and verifying that a sink device is authorized to receive the protected content in response to the comparison.

The portions of Graunke cited by the Office Action as corresponding to the receiving of the approval code (deriving the verification value in block 209), and the determining a local code (deriving the verification value in block 2080, actually describes a process for confirming that the deciphering is being properly performed by the sink device 104. In this regard Graunke teaches that a sink device generates a verification value in a predetermined manner and transmits those verification value to the source device, which also generates the verification values and compares the generated value with those received from the sink device. The comparison of the verification values allows the source device to determine and confirm that the **ciphered content is being properly deciphered** by the sink device (col. 3, lines 43-56). However, this process has nothing to do with authenticating access for the sink device, or verifying that the sink device is authorized to receive the protected content from the source device.

In fact, Graunke explicitly states that the process of generating the verification values by the source device is in **an integral part of ciphering** the video content, and the process of generating the verification values by the sink device is an **integral part of deciphering** the video content (col. 3, lines 43-50). Therefore, the sink device has presumably been already authenticated and it has been determined that the sink device is authorized to receive the video content, and the processes related to the generating and comparing of the verification values are not related at all to verifying that the sink device is authorized to receive the video content. In view of the above, applicants submit that Graunke fails to disclose or suggest notable features of amended claim 1, and as such, amended claim 1, and the claims that depend therefrom, are not anticipated by Graunke.

Amended claims 5, 17, 19, and 21 similarly recite the feature of comparing codes and verifying that a sink device is authorized to receive the protected content in response to the comparison. Thus, Applicants submit that amended claims 5, 17, 19, and 21, and the claims that depend therefrom, are not anticipated by Graunke for at least the same reasons as those discussed with respect to amended claim 1.

Amended claim 13 is directed to an alternative embodiment, and provides the feature of comparing an identifier associated with the sink device with a set of security key to authenticate access for the sink device. Specifically, amended claim 13 recites:

> ... comparing said identifier with said plurality of security keys and verifying that said second device is **authorized to receive said protected content in response to the comparison**, and selecting one of said plurality of security keys associated with said identifier using said first device ... (emphasis added)

Again, for the reasons discussed above, applicants submit that Graunke fails to disclose or suggest the recited step of verifying that the second device is authorized to receive the protected content by comparing the recited elements. Rather, the portions of Graunke cited by the Office Action describe a process of generating a common authentication key between the source device and the sink device using identifiers associated with, and exchanged between, the source device and the sink device. Specifically, the source device sums the private keys of its provided array indexed by the identifier of the sink device to generate the authentication key Km, and the sink device sums the private keys of its provided array indexed by the identifier of the sink device to generate the authentication key

Km. If the devices are authorized device, they will have generated and possess a common authentication key Km. However, nowhere does Graunke disclose or suggest the step of **comparing** a received identifier with a set of security keys **to verify** that the sink device is authorized to receive the protected content. Rather, according to Graunke, the source device and sink device independently generate the authentication key by summing the provided keys indexed by the received identifier. Therefore, applicants submit that Graunke fails to disclose each and every limitation of claim 13, and as such, amended claim 13, and the claims that depend therefrom, are not anticipated by Graunke.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

DAVID JAY DUFFIELD et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: 4/27/06

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia, 22313-1450 on:

April 27, 2006
Date

Lori Klewin
Lori Klewin